Computing the n-th coefficient of an algebraic power series modulo p in $O(\log n)$ operations

Martin Klazar*

May 19, 2016

Abstract

This is an exposition, for pedagogical purposes, of the formal power series proof of Bostan, Christol and Dumas [3] of the result stated in the title (a corollary of the Christol theorem).

Introduction

The generating function $c = c(x) = \sum_{n\geq 1} c_n x^n$ of the Catalan numbers $c_n = \frac{1}{n}\binom{2n-2}{n-1} = 1, 1, 2, 5, 14, 42, \ldots$ satisfies the quadratic equation

$$c = c^2 + x\ .$$

Can we effectively determine parity of c_n? Very easily: modulo 2 one has

$$c(x) = c(x)^2 + x \equiv c(x^2) + x$$

(by Lemma C below), and therefore $c_n \equiv c_{n/2}$ mod 2 for $n > 1$ and $c_1 \equiv 1$ mod 2 ($c_{n/2} = 0$ if $n/2 \notin \mathbb{N}_0$). Hence

$$c_n \equiv 1 \text{ mod } 2 \text{ for } n = 2^m,\ m \in \mathbb{N}_0, \text{ and } c_n \equiv 0 \text{ mod } 2 \text{ else}\,.$$

And c_n modulo 3 or modulo other prime p? An answer to this is provided much more generally by the *Christol theorem*, proved by Christol [5] for $q = 2$ and by Christol, Kamae, Mendès France and Rauzy [6] for any prime power q (see also Allouche and Shallit [1, Theorem 12.2.5]): a power series $f(x) \in F_q[[x]]$ is algebraic over $F_q(x)$ if and only if one can generate its coefficients $f_0, f_1, \ldots$ by a DFAO (a deterministic finite automaton with output that reads the $l+1$ digits of the q-adic expansion $n = (n_l \ldots n_1 n_0)_q$ and outputs f_n, we give one example in Concluding remarks). It is immediate from the Christol theorem that one can compute the nth coefficient of an algebraic power series in $F_q[[x]]$ in $O(\log n)$ arithmetic operations because n has $O(\log n)$ q-adic digits.

*klazar@kam.mff.cuni.cz

This write-up is an exposition of the proof of this result, stated as Theorem A below, that was given by means of power series in the recent preprint of Bostan, Christol and Dumas [3]. I promised in my course ‘Kombinatorické počítání’ (taught in this summer semester 2015/16) to supplement my unfortunately not very clear oral presentation of (something like) Theorem A with a written one — here it is.

Algebraic power series in $F_p[[x]]$

First we review some notation and notions from algebra. Puiseux series $K((x))_P$ and their order are only used at the end in Proposition H that is not needed to prove Theorem A. $\mathbb{N} = \{1, 2, \dots\}$, $\mathbb{N}_0 = \{0, 1, \dots\}$, $\mathbb{Z}$ is the ring of integers, $F_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is the finite p-element field where p is a prime number, and $[x^n]f$ denotes the coefficient of x^n in f. For $p \in \mathbb{N}$, $p \geq 2$, the p-adic expansion $m = (m_l \dots m_1 m_0)_p$ of $m \in \mathbb{N}_0$ is given by the unique expression $m = \sum_{i=0}^{l} m_i p^i$ where $m_i \in \{0, 1, \dots, p-1\}$ and (for $m > 0$) $m_l \neq 0$; $0 = (0)_p$. Let K be a field or an integral domain. For a field we denote by $\overline{K}$ its algebraic closure (e.g. $\overline{\mathbb{R}} = \mathbb{C}$ or $\overline{\mathbb{Q}}$ are the algebraic numbers). We denote by $K[[x]] \subset K((x)) \subset K((x))_P$, respectively, the ring of power series and the fields of Laurent series and Puiseux series with coefficients in K. Their elements are the formal series (we treat here all power etc. series formally) $\sum_{n \geq k} a_{n/d} x^{n/d}$, $a_{n/d} \in K$, where $k = 0$ and $d = 1$ for p. s., $k \in \mathbb{Z}$ and $d = 1$ for L. s., and $k \in \mathbb{Z}$ and $d \in \mathbb{N}$ for P. s. For $f = f(x) \in K((x))$ we use notation $f_n := [x^n]f(x)$. From the algebraic point of view, $K((x))$ is the field of fractions of $K[[x]]$ and for K of characteristic 0 (e.g. $K = \mathbb{Q}$) $\overline{K}((x))_P$ is the algebraic closure of $K((x))$. Thus in $\overline{K}((x))_P$ every polynomial with coefficients in $K((x))$ has a root. Recall that $K[x] \subset K(x)$ is, respectively, the ring of polynomials with coefficients in K and its field of fractions ($K(x)$ are the rational ‘functions’ over K). In fact, $K(x)$ is naturally a subfield of $K((x))$ and $K[x]$ a subring of $K[[x]]$. By $\deg a$, $a \in K[x]$, we denote the degree of a polynomial and by $\deg_y a$, $a \in K[x, y]$, the degree $\deg a$ when a is understood as $a \in K[x][y]$. By $\mathrm{ord}\, f$, $f \in K((x))_P$, we denote the order of f, the minimum n/d such that $a_{n/d} \neq 0$. We set $\deg 0 = -\infty$ and $\mathrm{ord}\, 0 = +\infty$. For any $f, g \in K((x))_P$ one has $\mathrm{ord}\,(fg) = \mathrm{ord}\, f + \mathrm{ord}\, g$ and $\mathrm{ord}\,(f + g) \geq \min(\mathrm{ord}\, f, \mathrm{ord}\, g)$, with equality if $\mathrm{ord}\, f \neq \mathrm{ord}\, g$. Similarly, for any $f, g \in K[x]$ one has $\deg(fg) = \deg f + \deg g$ and $\deg(f + g) \leq \max(\deg f, \deg g)$, with equality if $\deg f \neq \deg g$.

We state the basic result on computing coefficients of an algebraic power series in $F_p[[x]]$ (this is essentially proven in [6] but the formulation below is ours).

Theorem A ([6], 1980). *Suppose that p is prime, $P \in \mathbb{Z}[x, y]$ is a nonzero polynomial, $f = f_0 + f_1 x + f_2 x^2 + \cdots \in \mathbb{Z}[[x]]$ is a power series satisfying $P(x, f(x)) = 0$, and*

$$h = (d + 1)(p^d - d + 1) \deg_x P \quad \textit{where} \quad d = \deg_y P \ (\geq 1) \ .$$

Then from given $p, P, f_0, f_1, \dots, f_h$ one can construct an algorithm (actually a

DFAO) that computes

$$n \mapsto f_n \bmod p$$

in $O(\log n)$ *arithmetic operations* ($n \ge 2$).

But which operations exactly? These are arithmetic operations $(+, -, \times, :)$ in the field F_p and the operation of division with remainder in the ring $\mathbb{Z}$. By 'one can construct' here and below we mean that the task can be performed constructively (i.e. the algorithms or objects not merely exist but exist effectively). Theorem A follows from the following more specific result (again the formulation is ours).

Theorem B ([3]). *Let p, P, f, and h be as in Theorem A. We denote the mod p reduction of f again by $f \in F_p[[x]]$. Then from given $p, P, f_0, f_1, \dots, f_h$ one can construct polynomials $a, c \in F_p[x]$, a number $e \in \mathbb{N}$, a row $u \in F_p^{1\times e}$, p matrices $A_0, A_1, \dots, A_{p-1} \in F_p^{e\times e}$, and a column $v \in F_p^{e\times 1}$ such that for any $n \in \mathbb{N}_0$ one has*

$$\begin{aligned}
[x^n]f(x) \quad &= \quad f_n = [x^n](c(x) + a(x)h(x)) \quad \textit{where} \\
&\quad\; h(x) = \sum_{m=0}^{\infty} (uA_{m_l} \dots A_{m_1} A_{m_0} v) x^m \in F_p[[x]]
\end{aligned}$$

($m = (m_l \dots m_1 m_0)_p$ is the p-adic expansion of m).

Polynomial P in Theorem A in general does not determine unique power series solution $y = f(x)$ of $P(x, y) = 0$, e.g. $y^2 - x^2 = 0$ has two solutions $y = x$ and $y = -x$. One can introduce restrictions, for example to require that $P(0, 0) = 0$, $P_y(0, 0) \ne 0$, and $f(0) = 0$, producing unique solution, but we want result for completely general P. So to determine $f(x)$ we need to know a few initial coefficients, which is captured by the parameter h in Theorems A and B. Bounds on h are considered in Corollary G and Proposition H.

Let us see how Theorem B implies Theorem A. We are given a prime p, a nonzero $P \in \mathbb{Z}[x, y]$, and first few coefficients $f_0, f_1, \dots, f_h$ of a solution $y = f(x) \in \mathbb{Z}[[x]]$ of the equation $P(x, y) = 0$, where h is as in Theorem A. (We assume this is an honest input, $f_0, f_1, \dots, f_h$ are really initial coefficients of a solution. We leave as an exercise for the reader to design an effective check that it is true.) Taking out the largest common factor of the coefficients of $P(x, y)$ we may assume that they are together coprime. Then reducing $P(x, f(x)) = 0$ modulo p we get the relation $E(x, f(x)) = 0$ where $E \in F_p[x, y]$ is the *nonzero* mod p reduction of P and $f \in F_p[[x]]$ denotes again the mod p reduction of f — its coefficients f_n we want to compute. We do it by Theorem B. We construct in $O_{p,P}(1)$ operations the objects $a, c, e, u, A_0, A_1, \dots, A_{p-1}$, and v. For given $n \in \mathbb{N}_0$ we compute f_n as

$$f_n = [x^n]c(x) + \sum_{m=n-\deg a}^{n} [x^{n-m}]a(x) \cdot uA_{m_l} \dots A_{m_1} A_{m_0} v$$

where $m = (m_l \dots m_1 m_0)_p$. For each m (> 0) in the summation range it takes $l + 1 = l(m) + 1 = \lfloor \log_p m \rfloor + 1$ operations in $\mathbb{Z}$ (divisions by p with remainder) to determine its p-adic expansion. It takes $l+1$ matrix times column multiplications, one row times column multiplication, and one scalar multiplication (in F_p) to evaluate the summand. So we evaluate f_n in

$$\sum_{m=n-\deg a}^{n} (l(m)+1+(l(m)+1)e(2e-1)+2e+1) = O((\deg a)e^2 \log_p n)$$

operations. Altogether we need

$$O_{p,P}(1) + O((\deg a)e^2 \log_p n) = O_{p,P}(\log n)$$

operations ($n \geq 2$).

Proof of Theorem B

We start with four lemmas. Lemma C is well known and is crucial for the existence of the algorithm of Theorem A, and in fact for the all algebra (and analysis) in characteristic p.

Lemma C. *If p is prime and $z \in F_p((x))$ is any Laurent series then $z(x)^p = z(x^p)$. Consequently, for any $k \in \mathbb{N}_0$ one has*

$$z(x)^{p^k} = z(x^{p^k})\ .$$

Proof. Let $z(x) = z_r x^r + z_{r+1}x^{r+1} + \cdots$. Since $a^p = a$ for any $a \in F_p$ and $(u+v)^p = u^p + v^p$ for any $u, v \in F_p((x))$ (because $\binom{p}{i} \equiv 0 \bmod p$ for $0 < i < p$), we indeed have

$$\begin{aligned} z(x)^p &= z_r x^{pr} + (z_{r+1}x^{r+1} + \dots)^p \\ &= z_r x^{pr} + z_{r+1}x^{p(r+1)} + (z_{r+2}x^{r+2} + \dots)^p \\ &\vdots \\ &= z(x^p)\ . \end{aligned}$$

□

We define operators $S_r :\ F_p[[x]] \to F_p[[x]]$, $r \in \{0, 1, \dots, p-1\}$, by

$$S_r z(x) = S_r(z(x)) = S_r(\textstyle\sum_{n\geq 0} z_n x^n) = \sum_{n\geq 0} z_{pn+r}x^n\ .$$

Thus $S_r z(x)$ arises from $z(x)$ by taking only terms $z_n x^n$ with $n \equiv r$ modulo p and replacing the n in the exponent with $(n-r)/p$.

Lemma D ([3]). *Operators S_r have the following properties.*

1. *Linearity, $S_r(au+bv) = aS_r(u) + bS_r(v)$ for any $a, b \in F_p$ and $u, v \in F_p[[x]]$.*

2. $S_r(uv) = \sum_{s+t\equiv r \bmod p} x^{\lfloor (s+t)/p \rfloor} S_s(u)S_t(v)$ *for any* $u, v \in F_p[[x]]$*.*

3. $S_r(u(x)v(x^p)) = S_r(u(x))v(x)$ *for any* $u, v \in F_p[[x]]$*.*

4. If $u \in F_p[[x]]$ *and* $n = (n_l \dots n_1 n_0)_p \in \mathbb{N}_0$ *then*

$$u_n = [x^n]u(x) = (S_{n_l} \dots S_{n_1} S_{n_0} u(x))(0) = [x^0]S_{n_l} \dots S_{n_1} S_{n_0} u(x) \ .$$

5. For any $0 \neq u \in F_p[[x]]$ *there is an* $r \in \{0, 1, \dots, p-1\}$ *such that* $S_r u \neq 0$*.*

6. $S_r F_p[x] \subset F_p[x]$ *and* $\deg S_r a \leq (\deg a)/p$ *for any* $a \in F_p[x]$*.*

Proof. 1. This is immediate from the definition.

2. We have

$$[x^n]S_r(uv) = \sum_{i+j=pn+r} u_i v_j = \sum_{l+m=n,n-1;s+t=r,r+p} u_{pl+s} v_{pm+t}$$

($i, j, l, m, n \in \mathbb{N}_0$, $r, s, t \in \{0, 1, \dots, p-1\}$). The last sum equals the coefficient of x^n in the sum stated in 2.

3. This is a corollary of 2: $S_t(v(x^p))$ is the zero power series for $t \neq 0$ and $S_0(v(x^p)) = v(x)$.

4. Since ($r, s, r_i \in \{0, 1, \dots, p-1\}$)

$$S_r u(x) = \sum_{n\geq 0} u_{pn+r} x^n, \ S_s S_r u(x) = \sum_{n\geq 0} u_{p(pn+s)+r} x^n = \sum_{n\geq 0} u_{p^2 n+ps+r} x^n$$

and so on, the constant term of $S_{r_l} \dots S_{r_1} S_{r_0} u(x)$ is just $u_{(r_l \dots r_1 r_0)_p}$.

5. By the definition of S_r, for r one may take the least significant p-adic digit of any $n \in \mathbb{N}_0$ for which $u_n = [x^n]u \neq 0$.

6. Clear from the definition of S_r. □

Lemma E. *Let* K *be any field. If* $v_1, \dots, v_{d+1} \in K[x]^d$ *are* $d+1$ d*-tuples whose entries have degrees at most* $c \in \mathbb{N}_0$*, then one can construct coefficients* $d_1, \dots, d_{d+1} \in K[x]$*, not all* 0*, such that*

$$\sum_{i=1}^{d+1} d_i v_i = (0, 0, \dots, 0)$$

and $\deg d_i \leq dc$ *for every* $i = 1, \dots, d+1$*.*

Proof. Let $M \in K[x]^{(d+1)\times d}$ be the matrix with rows $v_1, \dots, v_{d+1}$. We may assume that it has full rank d, its columns are linearly independent over $K(x)$. (If not, we find by standard linear algebra some maximal index set $I \subset \{1, 2, \dots, d\}$ of linearly independent columns and solve the problem for restrictions of the tuples v_i to coordinates with indices in I). We find d row indices $I \subset \{1, 2, \dots, d+1\}$ such that $\det M_I \neq 0$, where M_I arises from M by deleting the row j not in

I ($[d+1]\backslash I=\{j\}$). The displayed equation can be written as (we replace d_i by x_i)

$$(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_{d+1})M_I=-x_jv_j\ .$$

We set $x_j=1$ and solve this linear system for the x_i, $i\in I$. By Cramer's rule, the solution is $x_i=\pm\det N_i/\det M_I$, $i\in I$, where N_i arises from M_I by replacing the row i with the row $-x_jv_j=-v_j$ (the determinants are in $K[x]$). From the definition of determinant and bound on degrees of the entries in M_I and N_i we get that $\deg\det N_i,\deg\det M_I\le dc$. Thus the desired coefficients are $d_j=\det M_I$ and $d_i=\pm\det N_i$, $i\in I$. Then $\deg d_i\le dc$ for every $i=1,\ldots,d+1$ and $d_j\ne 0$. □

Lemma F. *Let p be prime, $0\ne E\in F_p[x,y]$, $d=\deg_y E$, and let $f\in F_p[[x]]$ satisfy $E(x,f(x))=0$ (so $d\ge 1$). Then from given polynomial E one can construct polynomials $c_0,c_1,\ldots,c_k\in F_p[x]$, $0\le k\le d$, such that we have equation*

$$\sum_{i=0}^{k}c_i(x)f(x^{p^i})=0\ ,$$

$c_0\ne 0$, and $\deg c_0\le(d+1)(p^d-d+1)\deg_x E$.

Proof. We have $a_df^d=\sum_{i=0}^{d-1}a_if^i$ where $a_i=[y^i]E\in F_p[x]$ and $a_d\ne 0$. It follows that for given E, $0\le i\le d$, and $n\in\mathbb{N}_0$ one can construct polynomials $a_{i,n}\in F_p[x]$ such that

$$a_{d,n}f^n=\textstyle\sum_{i=0}^{d-1}a_{i,n}f^i,\ a_{d,n}\ne 0\ .$$

Thus the $d+1$ elements $f^{p^i}=f(x^{p^i})$ (Lemma C), $i=0,1,\ldots,d$, are linearly dependent over $F_p(x)$ and one can construct the dependency relation

$$\textstyle\sum_{i=0}^{d}d_i(x)f(x^{p^i})=0$$

with $d_i\in F_p[x]$ that are not all zero. Let $j\in\mathbb{N}_0$ be minimum with $d_j\ne 0$. Using Lemma D.5, we can construct $r_1,\ldots,r_{j-1}\in\{0,1,\ldots,p-1\}$ such that $S_{r_1}\ldots S_{r_{j-1}}d_j(x)\ne 0$. Applying $S_{r_1}\ldots S_{r_{j-1}}$ on the dependency relation and using Lemma D.3 we get the desired equation

$$\textstyle\sum_{i=j}^{d}(S_{r_1}\ldots S_{r_{j-1}}d_i(x))f(x^{p^{i-j}})=0\ .$$

We set $c_i=S_{r_1}\ldots S_{r_{j-1}}d_{i+j}(x)$, $i=0,1,\ldots,k=d-j$, and have $c_0=S_{r_1}\ldots S_{r_{j-1}}d_j(x)\ne 0$.

We derive the upper bound on $\deg c_0$. Since S_r does not increase degree, $\deg c_0\le\max_i\deg d_i$. We have this recurrence for the polynomials $a_{i,n}$: $a_{d,n}=1$ and $a_{i,n}=\delta_{i,n}$ for $0\le i,n\le d-1$, $a_{i,d}=a_i$ for $0\le i\le d$, and, for $n>d$, $a_{d,n}=a_{d,n-1}a_d=a_d^{n-d+1}$ and $a_{i,n}=a_{d-1,n-1}a_i+a_{i-1,n-1}a_d$ for $0\le i\le d-1$, with $a_{-1,n-1}=0$. Clearly, $\max_{0\le i\le d}\deg a_i=\deg_x E$. Using the recurrence and induction we get the bound $\max_i\deg a_{i,n}=0$ for $n=0,1,\ldots,d-$

1, $\max_i \deg a_{i,d} = \deg_x E$, and $\max_i \deg a_{i,n} \le (n-d+1)\deg_x E$ for $n \ge d$. Applying Lemma E on the $d{+}1$ d-tuples $(a_{i,n} \mid 0 \le i \le d{-}1)$, $n = 1, p, p^2, \dots, p^d$, we get $d_i \in F_p[x]$ in the dependency relation with $\max_i \deg d_i \le (d+1)(p^d - d+1)\deg_x E$. □

The lemma is inspired by Lemma 12.2.3 in Allouche and Shallit [1]. Equations of this type are called Mahler equations, after the German–British mathematician Kurt Mahler (1903–1988) who used them to prove transcendence of various numbers.

We start the proof of Theorem B proper. Let $0 \ne E \in F_p[x,y]$ be the mod p reduction of $P(x,y)$ (with coprime coefficients) and $d = \deg_y E \ge 1$. Since $E(x,f) = 0$, by Lemma F one can construct a Mahler equation

$$c_0(x)f(x) + c_1(x)f(x^p) + \cdots + c_k(x)f(x^{p^k}) = 0$$

for $f(x)$ where $c_i \in F_p[x]$, $k \le d$, $c_0(x) \ne 0$, and $\deg c_0 \le (d+1)(p^d - d + 1)\deg_x E \le h$ (h is as in Theorem A). We change the variable $f(x)$ to $g(x)$ by $f(x) = c_0(x)g(x)$. Using Lemma C and dividing by $c_0(x)^2$, we get a Mahler equation for $g(x)$,

$$g(x) + c_1(x)c_0(x)^{p-2}g(x^p) + \cdots + c_k(x)c_0(x)^{p^k-2}g(x^{p^k}) = 0$$

— now the new coefficient c_0 is 1. The small price we paid is that in general $g(x)$ is not a power series but $g(x) \in F_p((x))$. We write

$$g(x) = \sum_{n<0} g_n x^n + \sum_{n \ge 0} g_n x^n =: g_-(x) + h(x) \;,$$

$g_- \in x^{-1}F_p[x^{-1}]$ and $h \in F_p[[x]]$ (this is the $h(x)$ of Theorem B). Denoting the Mahler equation for $g(x)$ as $L(x,M)g(x) = 0$ (here $L(x,M)$ is a skew polynomial in x and the operator $M:\ u(x) \mapsto u(x)^p = u(x^p)$) we get effectively a Mahler equation for the power series $h(x)$,

$$L(x,M)h(x) = -L(x,M)g_-(x) =: b(x)$$

or more explicitly

$$h(x) + c_1(x)c_0(x)^{p-2}h(x^p) + \cdots + c_k(x)c_0(x)^{p^k-2}h(x^{p^k}) = b(x) \;.$$

Necessarily $b(x) \in F_p[x]$ because $b(x) = -L(x,M)g_-(x) \in F_p[x^{-1}, x]$ but also $b(x) = L(x,M)h(x) \in F_p[[x]]$. We write the equation as

$$h(x) = b(x) + d_1(x)h(x^p) + \cdots + d_k(x)h(x^{p^k})$$

where $b(x), d_i(x) := -c_i(x)c_0(x)^{p^i-2} \in F_p[x]$. Let $D := \max(\deg b, \deg d_i, 1 \le i \le k)$ and $h_{(i)} := h(x^{p^i})$. We consider the vector space

$$V := \{\alpha + \beta_0 h_{(0)} + \cdots + \beta_k h_{(k)} \mid \alpha, \beta_i \in F_p[x], \deg\alpha, \deg\beta_i \le D\}$$

over F_p. Clearly, $h(x) = h_{(0)} \in V$. It follows that $S_r(V) \subset V$ for each of the p operators S_r: using the equation for $h(x)$ and Lemma D.3 (and D.1) we have

$$\begin{aligned} & S_r(\alpha + \beta_0 h_{(0)} + \cdots + \beta_k h_{(k)}) = S_r(\alpha + \beta_0 b + \textstyle\sum_{i=1}^k (\beta_0 d_i + \beta_i) h_{(i)}) \\ & = S_r(\alpha + \beta_0 b) + \textstyle\sum_{i=1}^k S_r(\beta_0 d_i + \beta_i) h_{(i-1)} \end{aligned}$$

and $\deg S_r(\alpha + \beta_0 b), \deg S_r(\beta_0 d_i + \beta_i) \le \deg(\alpha + \beta_0 b)/p, \deg(\beta_0 d_i + \beta_i)/p \le 2D/p \le D$ (Lemma D.6). The $(D+1)(k+2)$-element set

$$B := \{x^j, x^j h_{(i)} = x^j h(x^{p^i}) \mid 0 \le j \le D, 0 \le i \le k\}$$

is a generating set for V — the linear span of B over F_p is V (but B is not a basis for V, as stated in [3]; $h_{(0)}$ is a linear combination of other elements of B). We set $e := (D+1)(k+2)$ and by fixing an ordering of B make it a tuple $B = (b_1, \ldots, b_e)$. We set $v \in F_p^{e \times 1}$ to be the column of coordinates of $h(x)$ in B (it has all 0s and one 1), $A_r \in F_p^{e \times e}$ for $r = 0, 1, \ldots, p-1$ to be the matrices of the operators S_r with respect to B (the j-th column of A_r lists the coordinates of $S_r(b_j)$ in B), and $u := (b_1(0), \ldots, b_e(0)) \in F_p^{1 \times e}$ to be the row of constant terms in B. Clearly we can obtain v, A_r, and u effectively. By Lemma D.4 and the definition of v, A_r, and u we have for any $n = (n_l \ldots n_1 n_0)_p \in \mathbb{N}_0$ that

$$h_n = [x^n]h(x) = [x^0] S_{n_l} \ldots S_{n_1} S_{n_0} h(x) = u A_{n_l} \ldots A_{n_1} A_{n_0} v \ .$$

Returning to $f(x)$ we see that

$$f(x) = c_0(x) g(x) = c_0(x) g_-(x) + c_0(x) h(x)$$

and set, finally, $c(x) := c_0(x) g_-(x)$ and $a(x) := c_0(x)$. It follows that $a, c \in F_p[x]$. How do we get $g_-(x)$? It is the negative part of $g(x) = f(x)/c_0(x)$. Since $\deg c_0 \le h$, we compute $g_-(x)$ from $c_0(x)$ and $f_0, f_1, \ldots, f_h$.

Let us review the computation. We are given p, P, and $f_0, f_1, \ldots, f_h$ (initial coefficients of a solution $y = f(x) \in \mathbb{Z}[[x]]$ to $P(x, y) = 0$, h is as given in Theorem A). Reducing P modulo p we get a nonzero $E \in F_p[x, y]$. From E we compute by Lemma F the coefficients $c_0, \ldots, c_k \in F_p[x]$, $c_0 \ne 0$, $\deg c_0 \le h$, and $k \le \deg_y E$, of a Mahler equation for $f(x)$. We compute $g_-(x) \in x^{-1} F_p[x^{-1}]$ as the negative part of $(f_0 + f_1 x + \cdots + f_h x^h)/c_0(x)$. Thus we have $L(x, M) = M^0 + \sum_{i=1}^k c_i(x) c_0(x)^{p^i - 2} M^i$ (the Mahler equation for $g(x)$) and compute $b(x) = -L(x, M) g_-(x) \in F_p[x]$. We have $K(x, M) := -\sum_{i=1}^k c_i(x) c_0(x)^{p^i - 2} M^i$ (the relation $h(x) = b(x) + K(x, M) h(x)$) and set $D = \max(\deg b, \deg_x K(x, M))$ and $e = (D+1)(k+2)$. We take the e-tuple

$$B = (x^j, x^j h(x^{p^i}) \mid 0 \le j \le D, 0 \le i \le k)$$

and compute the column v of coordinates of $h(x)$ in B (this is easy), the matrices $A_0, \ldots, A_{p-1}$ of the operators S_r with respect to B (S_r acts on x^j in the clear way, $S_r(x^j h(x^{p^i})) = S_r(x^j) h(x^{p^{i-1}})$ for $i > 0$, and for $i = 0$ we replace $h(x)$

with $b(x) + K(x, M)h(x)$), and the row u of constant terms in B (note that the constant term $h(0)$ is the constant term in $(f_0 + f_1x + \cdots + f_hx^h)/c_0(x)$). Finally, we compute $c(x) = c_0(x)g_-(x), a(x) = c_0(x) \in F_p[x]$. Thus we have computed $a, c, e, u, A_0, \ldots, A_{p-1}, v$, all we need to quickly evaluate f_n modulo p. We are done. □

Concluding remarks

An interesting problem is to locate the first different coefficient of two different power series solutions of the same polynomial equation. Theorem B yields the following corollary.

Corollary G. *If p is prime, $0 \neq E \in F_p[x, y]$, and $f, g \in F_p[[x]]$, $f \neq g$, satisfy $E(x, f(x)) = E(x, g(x)) = 0$, then*

$$f_n \neq g_n \ \ \textit{for some} \ \ n \le (d+1)(p^d - d + 1)\deg_x E,\ d = \deg_y E\ .$$

Another bound is given in

Proposition H. *If H is any field of characteristic 0, $0 \neq P \in H[x, y]$, and $f, g \in H[[x]]$, $f \neq g$, satisfy $P(x, f(x)) = P(x, g(x)) = 0$, then*

$$f_n \neq g_n \ \ \textit{for some} \ \ n \le \frac{d^2 + d - 4}{2}\deg_x P,\ d = \deg_y P\ .$$

Proof. We work with the fields $K = H(x) \subset H((x)) = L$ and the algebraic closure $M = \overline{L} = \overline{H}((x))_P$, the field of Puiseux series with coefficients in $\overline{H}$. There is a nonzero polynomial $Q \in H[x, y]$ such that Q divides P in $H[x, y]$, $Q(x, f(x)) = Q(x, g(x)) = 0$, and Q as $Q(y) \in K[y]$ has in M only simple roots. Indeed, write $P(y) = P_1(y)^{a_1}P_2(y)^{a_2}\ldots P_k(y)^{a_k}$ where each $P_i \in K[y]$ is irreducible (in $K[y]$), $a_i \in \mathbb{N}$, and no P_i divides other P_j, $i \neq j$. Irreducibility of the $P_i(y)$s implies as usual that they have in M only simple roots and do not share roots. By the Gauss lemma (Lang [7, Chapter IV.2]) we may take $P_i \in H[x][y]$. Hence we have $Q = P_i(y)$ where $P_i(f) = P_i(g) = 0$ or $Q = P_iP_j$, $i \neq j$, where $P_i(f) = P_j(g) = 0$.

Let $f_1 = f, f_2 = g, \ldots, f_d \in M$ be the (different) roots of $Q(y) = a_dy^d + \cdots + a_1y + a_0$, $a_i \in H[x]$ and $a_d \neq 0$, so $d = \deg_y Q \in \mathbb{N}$ (and $d \ge 2$). Let $e = \max_i \deg a_i = \deg_x Q \in \mathbb{N}_0$. From Vièta's formula $(-1)^i a_{d-i}/a_d = \sum_{1 \le j_1 < \cdots < j_i \le d} f_{j_1}\ldots f_{j_i}$ and properties of the ord function we get

$$\min_{1 \le i \le d} \operatorname{ord} f_i \ge \min_{0 \le i \le d} \operatorname{ord}(a_i/a_d) \ge -e\ .$$

We look at the order of the discriminant $D \in H[x]$ of $Q(y)$ (Lang [7, Chapter IV.6]),

$$D = a_d^{2d-2}\prod_{1 \le i < j \le d}(f_j - f_i)^2 =: (f - g)^2 E\ .$$

Since $Q(y)$ has no multiple root, D is a nonzero homogeneous polynomial in $a_0, a_1, \ldots, a_d$ with degree $2d-2$ and coefficients in $\mathbb{Z}$. So

$$\begin{aligned}2\,\mathrm{ord}\,(f-g) &= \mathrm{ord}\,D - \mathrm{ord}\,E \leq \deg D - \mathrm{ord}\,E \\ &\leq e(2d-2) - (2d-2)0 - 2(-e)(d(d-1)/2-1) \\ &= e(d^2+d-4)\end{aligned}$$

and, since $d \leq \deg_y P$ and $e \leq \deg_x P$, the stated bound follows. □

Alternatively, to determine uniquely an algebraic power series $f(x)$, instead of taking first few coefficients $f_0, f_1, \ldots, f_h$ and the polynomial equation $f(x)$ satisfies, one can represent $f(x)$ by a system of polynomial equations such that $f(x)$ is the first coordinate in the tuple of unique solutions to the system. Then one can effectively do some operations with algebraic power series in such representation (which applies in fact to multivariate power series), see Alonso, Castro-Jiménez and Hauser [2] for this interesting topic.

So how do the Catalan numbers c_n behave modulo 3? According to this DFAO (taken from the note of Rowland [8]):

$a_1 0 1 b_1$, $a_1 2 e_2$, $b_1 0 b_1$, $b_1 1 c_2$, $b_1 2 d_0$, $c_2 0 c_2$, $c_2 1 b_1$, $c_2 2 d_0$, $d_0 012 d_0$, $e_2 0 c_2$, $e_2 1 d_0$, $e_2 2 e_2$.

It has five states a_1, b_1, c_2, d_0, and e_2, with the output mod 3 residue in the index, and $5 \cdot 3 = 15$ transitions, with the input ternary digits written between the states. Computation starts always at a_1 and follows the ternary digits $n-1 = (t_l \ldots t_1 t_0)_3$, read from the least significant t_0. For example, $6-1 = (12)_3$ sends us in two steps from a_1 to d_0, and indeed $c_6 = 42$ is 0 mod 3.

For a bound on the number of states of the DFAO obtained from an algebraic power series see Bridy [4], and for further $f \in \mathbb{Z}[[x]]$ whose reduction f_n mod p (or mod p^k) can be computed by a DFAO see Rowland and Yassawi [9] (and the references therein).

Finally, we quote the two main results of Bostan, Christol and Dumas [3] which quantify the dependence of the complexity bound on P and p. Theorem 5 in [3] states:

> Let E be a polynomial in $F_p[x,y]_{h,d}$ such that $E(0,0) = 0$ and $E_y(0,0) \neq 0$, and let $f \in F_p[[x]]$ be its unique root with $f(0) = 0$. Algorithm 1 computes the Nth coefficient f_N of f using $\tilde{O}(d^3 h^2 p^{3d} \log N)$ operations in F_p.

Here h and d bound the x- and y-degree, respectively, and $\tilde{O}(\cdot)$ is $O(\cdot)$ with polylogarithmic factors omitted. Proof of this theorem we (roughly) followed in our expose. Another algorithm, considerably more efficient, is presented in Theorem 11 in [3]:

> Let E in $F_p[x,y]_{h,d}$ satisfy $E(0,0) = 0$ and $E_y(0,0) \neq 0$, and let $f \in F_p[[x]]$ be its unique root with $f(0) = 0$. One can compute the coefficient f_N of f in $h^2(d+h)^2 \log N + \tilde{O}(h(d+h)^5 p)$ operations in F_p.

References

[1] J.-P. Allouche and J. Shallit, *Automatic Sequences*, Cambridge University Press, Cambridge, 2003.

[2] M. E. Alonso, J. M. Castro-Jiménez and H. Hauser, Encoding algebraic power series, manuscript, 2014, 35 pages (available from H. H.'s homepage).

[3] A. Bostan, G. Christol and P. Dumas, Fast computation of the nth term of an algebraic series in positive characteristic, arXiv:1602.00545v1, February 2016, 8 pages.

[4] A. Bridy, Automatic sequences and curves over finite fields, ArXiv:1604.08241v1, April 2016, 22 pages.

[5] G. Christol, Ensembles presque périodiques k-reconnaissables, Theor. Comput. Sci. 9 (1979), 141–145.

[6] G. Christol, T. Kamae, M. Mendès France and G. Rauzy, Suites algébriques, automates et substitutions, Bull. Soc. Math. France 108 (1980), 401–419.

[7] S. Lang, *Algebra*, Springer, 2002 (revised 3rd edition).

[8] E. Rowland, What is … an automatic sequence?, Notices AMS, 62 (2015), 274–276.

[9] E. Rowland and R. Yassawi, Automatic congruences for diagonals of rational functions, J. Théor. Nombres Bordeaux 27 (2015), 245–288.

Charles University, KAM MFF UK, Malostranské nám. 25, 118 00 Praha, Czechia